Acquisition Directorate

Research & Development Center

Report No. CG-D-06-16

Maritime Cyber Security University Research

Phase I - Final Report

May 2016

Homeland Security

N O T I C E

This document is disseminated under the sponsorship of the Department of Homeland Security in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

Bert Macesker
Executive Director
United States Coast Guard
Research & Development Center
1 Chelsea Street
New London, CT 06320

Technical Report Documentation Page

1. Report No. CG-D-06-16		2. Government Accession Number	3. Recipient's Catalog No.
4. Title and Subtitle Maritime Cyber Security University Research: Phase I - Final Report			5. Report Date May 2016 6. Performing Organization Code Project No. 8501
7. Author(s) USCG Research and Development Center, Dennis Egan et al., Rutgers University, Nicole Drumhiller et al., American Military University, Adam Rose et al., University of Southern California; Milind Tambe, University of Southern California			8. Performing Report No. R&DC UDI # 1623
9. Performing Organization Name and Address	U.S. Coast Guard Research and Development Center 1 Chelsea Street New London, CT 06320		10. Work Unit No. (TRAIS) 11. Contract or Grant No. N/A
12. Sponsoring Organization Name and Address COMMANDANT (CG-FAC) US COAST GUARD STOP7501 2703 MARTIN LUTHER KING JR AVE SE WASHINGTON, DC 20593			13. Type of Report & Period Covered Final 14. Sponsoring Agency Code Commandant (CG-FAC) US Coast Guard Stop7501 Washington, DC 20593
15. Supplementary Notes The R&D Center's technical point of contact is Judith R Connelly, 860-271-2643, email: judith.r.connelly@uscg.mil			
16. Abstract (MAXIMUM 200 WORDS) Modern maritime systems are highly complex digital systems to ensure the safety and efficient operation of the shipping traffic so vital to the global economy. The vulnerabilities associated with reliance on digital systems in the maritime environment must be continuously examined. System protections must be ever ready to monitor vulnerabilities and secure maritime traffic systems. The U.S. Coast Guard must ensure the integrity of the entrances to our "digital ports" and work to develop practical cyber security solutions to protect the nation's maritime infrastructure.			
17. Key Words Cyber security, MTS, Risk Management, Threats, Vulnerabilities		18. Distribution Statement Distribution Statement A: Approved for public release; distribution is unlimited.	
19. Security Class (This Report) UNCLAS//Public	20. Security Class (This Page) UNCLAS//Public	21. No of Pages 18	22. Price

(This page intentionally left blank.)

EXECUTIVE SUMMARY

In 2013 the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. As of 2015, cyber terrorism remains the number one strategic threat. To remain the foremost authority on maritime security, the Coast Guard must "improve situational awareness of network operations and appropriately harden systems against cyber attacks" (USCG Cyber Implementation Plan v0.1).

In April 2015, the Rutgers University Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) DHS Center of Excellence hosted the Maritime Cyber Security Symposium which presented the U.S. Coast Guard's key cyber challenges. In June 2015 the USCG released the Cyber Strategy, a document that identifies three distinct strategic priorities that are critical to the Coast Guard's overall mission success - defending cyberspace, enabling operations, and protecting infrastructure.

On June 17, 2015 one day after the USCG Cyber Strategy release, the California Maritime Academy held the Maritime Cyber Security Research Summit to discuss maritime cyber security risks and vulnerabilities and to build upon the key challenges. A total of 76 participants attended the summit including 23 members of the USCG, 17 from state, local, and federal agencies, 15 maritime operators, and 21 from academia representing 16 universities. Three white papers, three presentations and a 16 page "Summary Report of Findings" representing a summation of each white paper were produced. In addition, three future research questions were identified by Rutgers CCICADA, American Military University (AMU), and the University of Southern California (USC) Center for Risk and Economic Analysis of Terrorism Events (CREATE) in conjunction with the USC Center for Interdisciplinary Decisions and Ethics **(**DECIDE).

This report represents the research, findings, and the conclusions formed by each university research group in an effort to assist the U.S. Coast Guard in operationalizing its maritime cyber strategy.

(This page intentionally left blank.)

TABLE OF CONTENTS

EXECUTIVE SUMMARY ..... **v**

LIST OF ACRONYMS AND ABBREVIATIONS ..... **viii**

1 BACKGROUND **1**

2 RESEARCH AREAS **2**

2.1 Rutgers CCICADA – Information Sharing Protocols Research Plan 2
2.2 American Military University – Risk Management Research Plan 3
2.3 USC CREATE - Threats and Vulnerabilities using Economic Modeling Research Plan 3
2.4 USC CREATE - Threats and Vulnerabilities using Game Theory Research Plan 3

3 RESEARCH RESULTS **4**

3.1 Rutgers CCICADA – Information Sharing Protocols Research 4
3.2 American Military University – Risk Management Research 6
3.3 USC CREATE – Threats and Vulnerabilities using Modeling and Simulation 7
3.4 USC CREATE – Threats and Vulnerabilities using Game Theory 8

4 CONCLUSION **8**

5 RECOMMENDATIONS **9**

APPENDICIES PROVIDED UNDER SEPARATE COVER

APPENDIX A. INFORMATION SHARING FOR MARITIME CYBER RISK MANAGEMENT

APPENDIX B. COVERING MARITIME CYBER SECURITY OBJECTIVE: HOW DO WE PROMOTE THE USE OF SOUND CYBER RISK MANAGEMENT PRINCIPLES?

APPENDIX C. ECONOMIC CONSEQUENCE ANALYSIS OF MARITIME CYBER THREATS

APPENDIX D. CYBER PROJECT AT USC

LIST OF ACRONYMS AND ABBREVIATIONS

AAPA	American Association of Port Authorities
AMSC	Area Maritime Security Committee
AMU	American Military University
ARL	Army Research Lab
BIMCO	Baltic and International Maritime Council
CCICADA	Command, Control and Interoperability Center for Advanced Data Analysis
CFR	Code of Federal Regulations
CJOS	Combined Joint Operations from the Sea
CREATE	Center for Risk and Economic Analysis of Terrorism Events
DCO	Deputy Commandant for Operations
DDOS	Distributed Denial of Service
DECIDE	Center for Interdisciplinary Decisions and Ethics
DETER	Defense Technology Experimental Research
E-CAT	Economic Consequences Analysis Tool
ECA	Economic Consequence Analysis
FS-ISAC	Financial Services Information Sharing and Analysis Center
MCSR	Maritime Cyber Security Research
MS-ISAC	Multi-State Information Sharing and Analysis Center
IMO	International Maritime Organization
ISAC	Information Sharing and Analysis Center
MCSS	Maritime Cyber Security Symposium
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
POMDP	Partially Observable Markov Decision Process
RDC	Research and Development Center
SEIM	Security Event Information Management
SQL	Structured Query Language
USC	University of Southern California
USCG	United States Coast Guard

1 BACKGROUND

In 2013 the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. As of 2015, cyber terrorism remains the number one strategic threat. If the Coast Guard is to remain the foremost authority on maritime security, it must "improve situational awareness of network operations and appropriately harden systems against cyber attacks" (USCG Cyber Implementation Plan v0.1).

In April 2015, the Rutgers University Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) DHS Center of Excellence hosted the Maritime Cyber Security Symposium (MCSS) which presented the U.S. Coast Guard's key cyber challenges. In June 2015 the USCG released the Cyber Strategy, a document that identifies three distinct strategic priorities that are critical to the Coast Guard's overall mission success - defending cyberspace, enabling operations, and protecting infrastructure.

After the USCG Cyber Strategy release, the California Maritime Academy held the Maritime Cyber Security Research (MCSR) Summit to discuss maritime cyber security risks and vulnerabilities and to build upon the key challenges. A total of 76 participants attended the summit including 23 members of the USCG, 17 from state, local, and federal agencies, 15 maritime operators, and 21 from academia representing 16 universities. Three white papers, three presentations and a 16 page "Summary Report of Findings" representing a summation of each white paper were produced. The purpose of the summit was to address the research challenge put forth by the USCG Deputy Commandant for Operations (CG-DCO) during the Maritime Cyber Security Symposium who challenged those present to help the USCG explore research areas and identify research priorities in an effort to better combat cyber threats, risks, and vulnerabilities in the Maritime Transportation System (MTS).

During the summit, six topics were identified by participants. These topics included:

1. Vulnerabilities: What analysis could be employed to identify the greatest cyber vulnerabilities in the maritime domain/MTS, both shipboard and ashore?
2. Resilience: What are the best options for operational and systems cyber resilience?
3. Threats: What analysis framework and tools could be used to map and predict dynamic maritime cyber threats?
4. Impacts: What framework should be employed for impact analysis for the MTS? What are the cascading consequences to the nation and economy of a cyber incident?
5. Critical Points: What approach should be used to conduct nodal analysis to identify single points of failure for maritime cyber events within the MTS, including navigation systems?
6. Info Sharing: How would a framework for network analysis be developed to support optimal information sharing with partners to address maritime cyber issues?

Following the summit, CG-DCO selected three research areas for further study concerning Maritime Cyber Security. Rutgers University, University of Southern California (USC), and American Military University (AMU) showed a willingness to explore these topics further. On August 31, 2015 the USCG Research and Development Center (RDC) was selected by the Chief of the Coast Guard's Office of Port and Facility Compliance to provide project oversight and to assist the teams in moving forward in their research areas.

2 RESEARCH AREAS

Three research areas were selected by CG-DCO for further study concerning Maritime Cyber Security. The questions and the university research assignments were as follows:

- Rutgers: Develop Information Sharing Protocols to meet the needs of industry and government.
- American Military University: Define sound cyber risk management principles.
- USC : Identify threats and vulnerabilities, and consider modeling and simulation to understand cyber impacts in the MTS.

2.1 Rutgers CCICADA – Information Sharing Protocols Research Plan

Rutgers University's Command, Control and Interoperability Center for Advanced Data Analysis (CCICADA) is a U.S. Department of Homeland Security University Center of Excellence (COE) that uses advanced data analysis and systems to address natural and manmade threats to the safety and security of the American people. The CCICADA group, led by Dr. Fred Roberts, recognized that the ability to share information in an effective and timely manner with all stakeholders in the Maritime Transportation System (MTS) is essential in keeping the MTS safe, secure, and resilient. As a result, the CCICADA team proposed to investigate methods to achieve rapid and useful information sharing in a way that both large and small players in the MTS could participate. In particular, they looked to investigate how larger content providers could be enticed to take the lead on information sharing.

The CCICADA group looked to first explore ways to incentivize environments that are both transparent and candid in the sharing of information. As part of the research, they also sought to categorize what information about the latest cyber threats and countermeasures should be shared, with whom, and at what rate of speed. To answer the question of speed of information distribution, they sought to understand the types of information that need to be shared rapidly as well as the types of information that do not pose an immediate threat. One example of information types included how and when to share reports on "near misses".

Organizational structures for information sharing between government and industry need to be better understood. For example,

- What information sharing leverage can be gained from existing organizations such as the Maritime Information Sharing and Analysis Center (ISAC) and Area Maritime Security Committees (AMSCs) or the National Cybersecurity and Communications Integration Center (NCCIC) or the International Maritime Organization (IMO) or NATO's Center for Combined Operations from the Sea?
- How is information sharing performed in other sectors such as those facilitating financial services, travel, utilities, and medical services?
- Can we find good systems for use of real-time machine to machine interfaces such as the Security Event Information Management (SEIM) software that can automatically collect, filter, vet, and distribute threat analysis and trends?

Finally, the group looked to analyze the role of the Coast Guard in cyber security information sharing; roles such as developing standards for sharing systems, exchanging best practices, or enforcing sharing regulations. The impetus behind this work was to translate existing USCG reporting procedures for physical security risks into good reporting procedures for cyber security risks.

2.2 American Military University – Risk Management Research Plan

American Military University (AMU) provides courses solely online. With over 100,000 students AMU is the number one provider of education to the military with just over 65,000 military students. Approximately 25% of the 3,933 USCG members who used Tuition Assistance in FY14 attended AMU. The strength of AMU's faculty is their designation as scholar-practitioners who were able to guide students in analyzing the risk management research through an independent study course.

AMU was tasked with researching the question: "How does the Coast Guard better promote the use of sound cyber risk management principles?" This question directly addresses the Commandant's resolve to protect infrastructure as identified in the United States Coast Guard Cyber Strategy released in June 2015.

The focus of AMU's proposed research was to address risk management at the individual company or vessel level, while taking into consideration both risk management and resilience. The team also planned to research risks arising from the confluence of physical and cyber threats by exploring the vulnerabilities that arise when interconnected technologies are breached, resulting in widespread damage.

2.3 USC CREATE - Threats and Vulnerabilities using Economic Modeling Research Plan

The University of Southern California hosts CREATE, the nation's first Department of Homeland Security Center of Excellence. CREATE has a long history of working with the USCG and other organizations. The USC CREATE team looked to investigate methods to assess cyber vulnerability and to assess mitigation strategies in the maritime cyber domain. To conduct this task, the team sought to determine what type of information can be used to assess cyber threats and vulnerability. This research would use publicly available information from various sources including reports on the latest cyber threats/attacks, maritime cyber-readiness, available intelligence, ship-to-shore communications, port operations, and probability encoding from cyber experts. The results of the information collection are used to create probability assessments for the most important cyber threats and scenarios.

The USC team also sought to provide a methodology for assessing the economic consequences of various cyber threats. CREATE's Economic Consequences Analysis Tool (E-CAT), which provides fast economic consequences of attacks, was to be extended to include cyber threats. Given probabilities of various cyber scenarios and their economic consequences, the team would then be able to determine a metric of cyber threat and a comprehensive framework for the estimation of total economic consequences of maritime cyber threats. This includes a categorization of threats and how threats directly affect port operations.

2.4 USC CREATE - Threats and Vulnerabilities using Game Theory Research Plan

The USC CREATE team also planned to identify exfiltration attacks using the Partially Observable Markov Decision Process (POMDP) decision making framework. Exfiltration attacks are the unauthorized access of systems and data through orchestrated, salient actions that mimic the normal behavior of authorized users.

Detectors of exfiltration attacks have a high false positive rate that is caused by legitimate traffic being misclassified as suspicious. The USC CREATE team planned to leverage additional information and better reasoning about the true state of the cyber-physical environment to identify whether or not exfiltration attacks are occurring.

3 RESEARCH RESULTS

3.1 Rutgers CCICADA – Information Sharing Protocols Research

Effective and timely sharing of cyber risk management information among all stakeholders in the Maritime Transportation System (MTS) is vital to maintaining a safe, secure and resilient MTS. To develop information sharing protocols across this complex system, the Coast Guard must consider the layers of cyber risk management, including communication and technology, economic, and legal and regulatory aspects. The research performed by Rutgers CCICADA addressed the following questions:

- What is the most appropriate role for the U.S. Coast Guard (USCG), and how does guidance for physical security relate to cyber risk management needs?
- What organizational systems could best support the needed sharing?
- What kinds of incentives could be used to encourage participation, particularly from private industry?
- What information needs to be shared, and when?
- What technologies could be used to enable and safeguard the information sharing?

The team identified that the problem of organizing for maritime cyber risk management may result from the distinct layers of concern - communications and technology arrangements, economic considerations, and legal and regulatory matters, that differ based on the needs of governments and their agencies, commercial shipping and cruise firms, the onboard captains and crew, and the ports and associated personnel. The white paper provided by the CCICADA-Rutgers research team (Appendix A) addressed these topical questions, the research process, and the team's initial findings based on the interviews conducted and documents read. This white paper is organized into five topical areas with a summation of each finding below:

- **The role of the USCG and extending physical security to cyber security - cyber risk management** discussed the need for the Coast Guard to develop high-level cyber risk management guidelines for facilities that are similar to the existing Code of Federal Regulations for maritime facilities (33CFR105). Existing documents that could be leveraged include the NIST framework, the NIST 800 series, the ISO/IEC series, Baltic and International Maritime Council (BIMCO) recommendations, and the Center for Internet Security (CIS) Controls for Effective Cyber Defense. The developed guidelines could be used to perform cyber risk management audits, establish performance-based standards and metrics to assess the meeting of those standards, specify training and gauge its effectiveness, and establish a common language that enables better communication with other government agencies in support of information sharing.

- **Organizational systems for information sharing** explored how partnering with effective national organizations can help the USCG organize systems for information sharing. Findings included having the Coast Guard partner with effective national organizations that include increasing its current one-person presence at the National Cybersecurity and Communications Integration Center (NCCIC) to expand opportunities to coordinate with NCCIC partners and report cyber risk management alerts, trends and mitigation strategies across the USCG, commercial partners, and other appropriate government agencies; redevelopment of the Maritime Information Sharing and Analysis Center (ISAC) to provide an industry-focused community for information sharing; enhancing cyber incident reporting capabilities to reduce confusion when non-classified level incidents occur and to support the sharing of information across agencies; use Area Maritime Security Committees (AMSCs) develop ways to communicate cyber issues to the large number of MTS entities without technical expertise; use resources and relationships and resources established through NATO's Combined Joint Operations from the Sea (CJOS), the American Association of Port Authorities (AAPA), and the International Maritime Organization (IMO) to ease the challenges of information sharing internationally.

- **Motivation and barriers for sharing information** explored ways to incentivize information sharing among key players in the MTS. It is important to provide incentives for sharing information as industry begins to take the initial steps that lead to enhanced maritime cyber risk management. Suggested motivators for information sharing included increased technical support, improved access to security information, and insurance rate reductions. Suggested negative incentives included regulations and penalties for non-reporting.

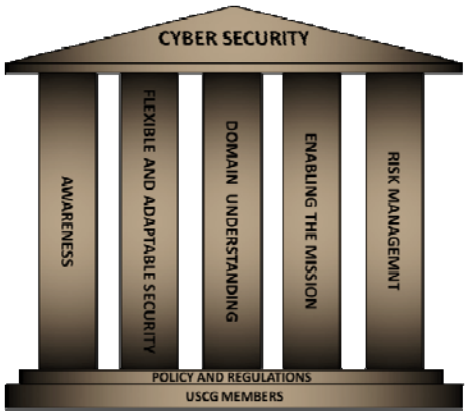
- The research team found that the **information to share, and what to share rapidly vs. slowly** could be based on the Cybersecurity Information Sharing Act of 2015 which identifies eight categories of cyber threats, and could be the framework of a strategy describing what to share regarding threats. Other methods could be based on the Financial Services Information Sharing and Analysis Center (FS-ISAC) which structures its sharing according to incidents, threats, vulnerabilities, and resolutions/solutions; the Multi-State Information Sharing and Analysis Center (MS-ISAC) where information shared would include vulnerabilities, operational cybersecurity information sharing techniques, botnet information, malicious IP addresses, near misses, incidents, threats, resolutions/solutions, and the seven key Netflow fields; sensitive information sharing could be done using a Red|Yellow|Green traffic light protocol where the current status is posted to the HOMEPORT portal.

- **Technologies that support information sharing** present several challenges due to resource limitations and needs that differ amongst the coordinating bodies. Those responsible must agree on protocols for reporting problems, attacks, and countermeasures in addition to receiving and filtering streams of information that must be prioritized, classified and prepared for controlled dissemination. In accordance with FS-ISAC, full implementation should not require vendor specific software and should instead rely on existing protocols and systems that should be evaluated to determine their ability to be used in the MTS.

The white paper concludes with a set of recommendations related to each topical area.

3.2 American Military University – Risk Management Research

American Military University (AMU) accepted the role of researching ways to promote the use of sound cyber risk management principles and presented their findings in a white paper titled *Covering Maritime Cyber Security Objective: How do we promote the use of sound cyber risk management principles?* (Appendix B). The AMU research team consisted of military, government, and civilian personnel. The team performed an extensive literature review to evaluate risks to the Coast Guard and ways these risks can be mitigated. The focus of the AMU team's research was based in the needs of the Coast Guard's fleet, potentially conflicting with the overarching security goals of the Coast Guard as a whole. Those in the field understand the need for information in real-time and place the ability to share data and the availability of data as a top priority. Conversely, the research team realized that the Coast Guard must also protect the information that is shared, their personnel, and the data necessary to carry out its missions.



The AMU team proposed a five-pillar approach to categorize risks. The foundation of the pillars is policy and regulations that are enacted by members of the MTS. The pillars are Awareness, Flexible and Adaptable Security, Domain Understanding, Enabling the Mission, and Risk Management.

- **Awareness** is the effective communication of the existing threats to members of the MTS. Awareness can be established through continuous education and training.
- **Flexible and Adaptive Security** allows participants at all levels to use scalable tactics to combat threats and minimize risks.
- **Domain Understanding** promotes an understanding of the threats that exist in the maritime domain.
- **Enabling the Mission** allows participants at all levels to cross share information while considering varying levels of information security that may be required.
- **Risk Management** represents the need to plan, manage, and establish thresholds for risks and threats.

The AMU research team moved beyond the identification and classification of risk mitigation to focus on ways the Coast Guard can promote sound practices in risk management. The team proposed both positive and negative motivators.

Positive motivators include:

- Recognition or awards.
- Designations / titles for those port partners educated and/or trained in cyber security's best practices.
- Praise / reward individuals that identify vulnerabilities and/or provide actionable solutions to threats.

Negative motivators include:

- Retraining in the form of courses or violator-led trainings for those who fail to follow procedures.
- Prosecution of violators.
- Discharge, job loss, civil lawsuits.

The AMU research team also identified environmental changes that could improve risk management practices to improve the overall port environment. These changes include:

- Mandating regular patch updates from all vendors and those who have access.
- Mandating information sharing of cyber attacks with partners who track and combat attacks.
- Enacting data monitoring and the disabling of access to those who pose high security risks.
- Creating quarantine zones that establish boundaries between internal and external networks.
- Automating the scanning of data that enters networks.
- Using fingerprint scans or facial recognition for system access instead of passwords.

In conclusion, the AMU research team performed literature reviews, interviews with industry and USCG entities to determine that the training of information technology professionals and security experts is essential in identifying new ways terrorists and criminals implement methods to hack systems. Learning these new advancements can help provide personnel with the knowledge needed to develop tools to combat cyber terrorism and cyber-criminal activity. The group also suggests that a new position of Cyber Security Officer be created to better train USCG personnel.

Moving forward, the AMU team suggests that the USCG works towards getting feedback from those in the maritime industry to formulate a comprehensive cyber security strategy that will streamline maritime defenses. Research led the team to conclude that this approach would enable better information sharing, make it easier to identify weaknesses, and potentially divert cyber attacks that could have crippling effects.

3.3 USC CREATE – Threats and Vulnerabilities using Modeling and Simulation

The USC CREATE research team investigated methods to assess cyber vulnerability and to assess mitigation strategies in the maritime cyber domain. The white paper provided (Appendix C) summarized the current state of the Economic Consequence Analysis (ECA) of maritime cyber threats. The research performed confirmed the feasibility of ECA in the overall U.S. Coast Guard's cyber strategy, and enabled the team to outline a framework for integrating the two. The document summarized the well-established CREATE ECA Framework and illustrated its application to prior studies of port disruptions. These studies have demonstrated the need for a comprehensive framework that includes proper attention, not only to standard features of traditional economic impact analysis, but also to aspects of resilience, behavioral linkages, and remediation of damages.

The white paper also presented a summary of the recently developed Economic Consequence Analysis Tool (E-CAT), which is intended to provide rapid estimates of economic losses from more than 30 types of threats, including those related to the cyber domain and transportation system disruptions. Finally, there is a summary of research on numerous resilience tactics applicable to the recovery from cyber threats.

The goal of USC CREATE's ongoing research is to incorporate into E-CAT the capability to rapidly estimate economic consequences of various maritime cyber threats. Maritime cyber threats and their characteristics will be determined in collaboration with the USCG. The E-CAT methodology will be adapted to the special needs of this objective. The product to be transitioned to the USCG will essentially be a decision-support capability that will enable high-level decision-makers to better allocate resources across numerous threats.

3.4 USC CREATE – Threats and Vulnerabilities using Game Theory

An 18-month effort funded by the Army Research Lab (ARL) is providing the USC CREATE research team the opportunity to research ways to protect USCG networks against data exfiltration - the unauthorized transfer of sensitive or critical information. Due to the high volume of network traffic that can closely resemble normal network activity, detecting and protecting against exfiltration attacks can be extremely difficult. Additionally, with these attacks it is possible to discretely transfer small amounts of data over long periods of time, meaning that any suspicious queries will not be immediately obvious.

To address the difficult problems posed by exfiltration attacks, the USC CREATE research team will wrap imperfect exfiltration detectors (and possibly other detectors such as malware detector) in a decision making framework known as a Partially Observable Markov Decision Process (POMDP). This dual layered analysis will then be able to leverage additional network information and better reason about the true state of the network and whether exfiltration is occurring. By modeling the network this way the team will also be able to determine best response actions based on the type of suspicious activity.

Once the system is able to accurately detect signs of data exfiltration from the background traffic (within an acceptable threshold of error), the team plans to assist network administrators in defending their networks. This will be done by expanding the capabilities of Defense Technology Experimental Research (DETER) using POMDP to include attacks that are trying to infiltrate a network from outside an organization. This portion of the project is motivated by the observation that an attack in progress often produces a series of suspicious events but not a single smoking gun where the defender must decide whether a serious threat exists and what an appropriate response is.

The simulation will be built in the DETER test bed operated by the USC Information Sciences Institute. Using the DETER test bed, this simulation will emulate an actual computer network, against which agents launch common attacks (SQL injection, DDoS, etc.). The decision aid will then be trained to recognize potential attacks and deploy defenses against them.

4 CONCLUSION

This report represents the research, findings, and the conclusions formed by each university research group in an effort to assist the U.S. Coast Guard in operationalizing its maritime cyber strategy. Rutgers CCICADA investigated information sharing protocols to meet the needs of industry and government. The white paper submitted by Rutgers CCICADA discussed the need for the Coast Guard to develop high-level cyber risk management guidelines for facilities; explored how partnering with effective national organizations can help the USCG organize systems for information sharing; explored ways to incentivize information sharing among key players in the MTS; suggested that the information shared and the speed of information sharing (rapid vs. slow) could be based on the Cybersecurity Information Sharing Act of 2015; and presented some of the challenges that arise due to conflicting needs of information sharing coordinating bodies. American Military University (AMU) accepted the role of researching ways to promote the use of sound cyber risk management principles. The AMU team proposed a five-pillar approach to categorize risks; proposed positive and negative motivators to promote sound practices in risk management; and identified changes that could improve risk management practices to improve the overall port environment. The USC CREATE research team investigated methods to assess cyber vulnerability and to assess mitigation strategies in the maritime cyber domain. The white paper by USC CREATE summarized the

current state of the economic consequences of maritime cyber threats; provided an overview of the recently developed Economic Consequence Analysis Tool (E-CAT); and summarized their research on numerous resilience tactics applicable to the recovery from cyber threats.

In conclusion, the overall findings of the university research teams promoted the goals set forth by the project and laid the foundation for further exploration of the topics of risk management, information sharing, threats and vulnerabilities in the MTS. Phase II of the project will be used to build on this knowledge and the information gathered during this phase. Upon completion, these phases will work together in support of the Coast Guard Cyber Strategy to improve situational awareness of network operations and appropriately harden MTS systems against cyber attacks.

5 RECOMMENDATIONS

RDC recommends that this work be pursued into Phase II of this project. Additional breadth and depth of cyber security research should be considered in both initial research and sustained efforts as part of overall USCG interests. Such follow-on approaches to this work could include:

- Risk Assessments - understanding what cyber risk assessments for ports, facilities, and vessels look like; what risk assessments should address; existing assessment models the USCG can borrow from; what a cyber inventory looks like; the scalable and functional steps that a survey conducted for cyber security assessments should include.
- Cyber Safety and Security Postures – actions vessel owners and port entity operators should perform to evaluate their cyber safety and security postures (perhaps within the context of MTSA); how can actions by port entity operators and vessel owners be validated; determining the validating authority for cyber compliance; methods to measure the effectiveness of a compliance regime; performance-based protection measures

In addition, RDC plans to continue collaboration with USC CREATE's development of the E-CAT and game theory capabilities as they relate to the maritime cyber domain.

(This page intentionally left blank.)